KING & SPALDING LLP

191 Peachtree Street
Atlanta, Georgia 30303-1763
Telephone: 404/572-4600
Facsimile: 404/572-5100
www.kslaw.com

FACSIMILE

Important Notice: This facsimile transmission is intended to be delivered only to the named addressee, and may contain material that is confidential, proprietary or subject to legal protection or privilege. If it is received by anyone other than the named addressee, the recipient should immediately notify the sender at the address and telephone number set forth herein and obtain instructions as to the disposal of the transmitted material. In no event should such material be read or retained by anyone other than the named addressee, except by express authority of the sender or the named addressee.

DATE: October 25, 2004

Recipient	Company	City/State	Telephone #	Fax #
Examiner Eric B. Kiss	U.S. Patent and Trademark Office	Arlington, VA	730-305-7737	703-872-9306

FROM: Steven P. Wigmore 5551 **Our Ref. #:** 05456.105041

NUMBER OF PAGES (Including Cover Page): 10

MESSAGE:

PLEASE CHECK THAT ALL PAGES ARE RECEIVED. IN CASE OF PROBLEMS, PLEASE CALL EVA H. VAN CAMP AT 404-572-2459.

ALL RETURN TELECOPY MESSAGES SHOULD BE SENT TO 404/572-5100. THANK YOU.

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Applicant Initiated Interview Request Form

Application No.: 09/642,625 First Named Applicant: Peter A. J. van der Mode
Examiner: Eric B. KISS Art Unit: 2122 Status of Application: Under Non-Final

Tentative Participants: (40,447)
(1) Steven P. Wigmore (2) Eric B Kiss

(3)________ (4)________

Proposed Date of Interview: 10/27/2004 WED Proposed Time: 2:00 (AM [✓ PM])

Type of Interview Requested:
(1) ☒ Telephonic (2) ☐ Personal (3) ☐ Video Conference

Exhibit To Be Shown or Demonstrated: ☒ YES ☐ NO
If yes, provide brief description: Proposed Claim amendment, See attached

Issues To Be Discussed

Issues (Rej., Obj., etc)	Claims/ Fig. #s	Prior Art	Discussed	Agreed	Not Agreed
(1) Rejection	1,11,18,20,22,26,29	UHSBT	☐	☐	☐
(2)			☐	☐	☐
(3)			☐	☐	☐
(4)			☐	☐	☐

☐ Continuation Sheet Attached

Brief Description of Arguments to be Presented:

The prior art of Record does not teach nor suggest building a new virtual machine that comprises a complete personal computer. The prior art also does not teach nor suggest tracking functions with flags and the sequence thereof.

An interview was conducted on the above-identified application on ________

NOTE:
This form should be completed by applicant and submitted to the examiner in advance of the interview (see MPEP § 713.01).
This application will not be delayed from issue because of applicant's failure to submit a written record of this interview. Therefore, applicant is advised to file a statement of the substance of this interview (37 CFR 1.133(b)) as soon as possible.

10/25/2004

Reg. No. 40,447
(Applicant/Applicant's Representative Signature)

(Examiner/SPE Signature)

This collection of information is required by 37 CFR 1.133. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 21 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND

Internet Security Systems, Inc. - 08286-105041
Draft Claim Amendment to be Sent to Examiner for Telephonic Interview
U.S. Patent Application Serial No. 09/642,625
Inventor: Peter A. J. Van Der Made
Filed: August 18, 2000
Computer Immune System and Method for Detecting Unwanted Code in a Computer System

1. (Currently Amended) A method for identifying presence of malicious code in program code within a computer system, the method comprising:

~~initializing~~ building a new virtual machine within the computer system by assigning fresh physical memory to a memory array each time a target program is to be executed, the memory array functioning as memory for the virtual machine, the virtual machine comprising a complete virtual personal computer (PC) implemented by software simulating functionality of a central processing unit, [[and]] memory, [[and]] a virtual operating system simulating functionality of a multi-threaded operating system of the computer system, input/output (I/O) ports, BIOS firmware, and data areas for the virtual operating system;

virtually executing [[a]] the target program within the virtual PC so that the target program interacts only with an instance of the virtual operating system;

analyzing behavior of the target program upon completion of virtual execution to identify an occurrence of malicious code behavior based upon an evaluation by the virtual machine of a behavior pattern representing information about all functions simulated by the target program during virtual execution; and

terminating the virtual PC after the analyzing process, thereby removing from the computer system a copy of the target program that was contained within the virtual PC so that the executed target program cannot affect performance of later executed programs.

11. (Currently Amended) A method for identifying presence of malicious code in program code within a computer system, the method comprising:

initializing a virtual machine within the computer system, the virtual machine comprising software simulating functionality of a central processing unit and memory and a virtual operating system simulating functionality of a multi-threaded operating system of the computer system;

virtually executing a target program with the virtual machine so that the target program interacts with an instance of the virtual operating system rather than with the operating system of the computer system, whereby the malicious code is fully executed during virtual execution of the target program if the target program comprises the malicious code;

generating a behavior pattern for the target program by tracking functions performed and not performed by the target program with flags in a behavior pattern field and by tracking a sequence in which the functions are called by the target program with the behavior pattern field in order to collect information about all functions simulated by the target program during virtual execution; and

terminating the virtual machine upon completion of the virtual execution of the target program, leaving behind a record of the behavior pattern that is representative of operations of the target program with the computer system, including operations of the malicious code if the target program comprises the malicious code.

18. (Currently Amended) A memory storage device comprising computer-executable steps for identifying the presence of malicious code in program code in a computer system, comprising:

~~initializing~~ building a new virtual machine for the computer system by assigning fresh physical memory to a memory array each time a target program is to be executed, the memory array functioning as memory for the virtual machine, the virtual machine comprising a complete virtual personal computer (PC) implemented by software simulating functionality of a central processing unit, [[and]] memory, [[and]] a virtual operating system simulating functionality of a multi-threaded operating system of the computer system, input/output (I/O) ports, BIOS firmware, and data areas for the virtual operating system;

executing a target program within the virtual PC so that the target program completes a virtual execution by interacting only with an instance of the virtual operating system;

generating a behavior pattern by completing virtual execution of the target program within the virtual PC, the behavior pattern representative of operational functions completed by the target program during virtual execution, including at least one of virtual operating system calls, Input/Output functions and program functions supported by the target program;

upon completion of virtual execution, operating the virtual machine to compare the behavior pattern generated by virtual execution of the target program to a behavior pattern representative of operations by the malicious code to identify an occurrence of malicious code behavior; and

in the event that the comparison process results in a match representing an identification of malicious code behavior by the target program, then identifying the target program as comprising the malicious code.

19. (Currently Amended) The memory storage device of Claim 18 further comprising the computer-executable step of removing the target program from the computer system in response to an identification of the target program comprising malicious code so that the target program cannot affect the performance of subsequent programs executed by the computer system.

20. (Currently Amended) A memory storage device comprising computer-executable steps for identifying the presence of malicious code in program code in a computer system, comprising:

executing a target program within a virtual personal computer (PC) so that the target program completes a virtual execution by interacting only with an instance of a virtual operating system, the virtual PC comprising software operative to simulate functionality of a processor and memory, the virtual operating system operative to simulate functionality of a multi-threaded operating system for the computer system, the virtual PC and the virtual operating system operating in combination to form a virtual machine;

collecting information about the behavior of the target program during virtual execution of the target program by the virtual machine by tracking functions performed and not performed by the target program with flags in a behavior pattern field and by tracking a sequence in which the functions are called by the target program with the behavior pattern field in order to create a record of virtual operations of the target program, whereby the record reflects a plurality of operations of the malicious code if the target program comprises the malicious code;

upon completion of virtual execution of the target program, analyzing the record with the virtual machine to identify an occurrence of malicious code behavior by comparing the record to a behavior pattern representative of the operations performed by the malicious code; and

in the event that the record matches the malicious code behavior, then identifying the target program as comprising the malicious code.

21. (Currently Amended) The memory storage device of Claim 20 further comprising the computer-executable step of removing the target program from the computer system in response to an identification of the target program comprising malicious code so that the target program cannot affect performance of subsequent programs executed by the computer system.

22. (Currently Amended) A computer-implemented method for identifying a presence of malicious code in program code for a computer system, comprising the steps:

building a new virtual machine for the computer system by assigning fresh physical memory to a memory array each time a target program is to be executed, the memory array functioning as memory for the virtual machine;

virtually executing [[a]] the target program within [[a]] the virtual machine comprising a complete virtual personal computer (PC) implemented by software operative to simulate functionality of a processor, [[and]] memory, [[and]] a virtual operating system having software simulating functionality of a multi-threaded operating system for the computer system, input/output (I/O) ports, BIOS firmware, and data areas for the virtual operating system, wherein virtual execution of the target program comprises interactions with an instance of the virtual operating system; and

creating a record of all functions simulated by the target program during virtual execution of the target program by the virtual machine, the record comprising a behavior pattern representative of the behavior of the target program as if it were executed on the computer system, the behavior pattern comprising characteristics of malicious code behavior in the event that the target program comprises the malicious code.

25. (Currently Amended) The computer-implemented method of Claim 24 further comprising the step of removing the target program from the computer system in response to an identification that the target program comprises the malicious code so that the target program cannot affect performance of subsequent programs executed by the computer system.

26. (Currently Amended) A memory storage device comprising computer-executable steps for identifying the presence of malicious code in program code in a computer system, comprising:

executing a target program within a virtual personal computer (PC) so that the target program completes a virtual execution by interacting only with an instance of a virtual operating system, the virtual PC comprising software operative to simulate functionality of a processor and memory, the virtual operating system operative to simulate functionality of a multi-threaded operating system for the computer system, the virtual PC and the virtual operating system operating in combination to form a virtual machine;

collecting information about the behavior of the target program in response to virtual execution of the target program by the virtual machine;

in response to completing virtual execution of the target program, collecting information about interrupt call operations that call any interrupt service routine modified by the virtual execution of the target program;

creating a record by tracking functions performed and not performed by the target program with flags in a behavior pattern field and by tracking a sequence in which the functions are called by the target program with the behavior pattern field, the functions comprising the interrupt call operations, the record comprising the information collected about the virtual execution of the target program and the interrupt call operations that call any interrupt service routine modified by the virtual execution of the target program;

analyzing the record to identify an occurrence of malicious code behavior by comparing the record to a behavior pattern representative of the operations performed by the malicious code; and

in the event that the record matches the malicious code behavior, then identifying the target program as comprising the malicious code.

27. (Currently Amended) The memory storage device of Claim 26 further comprising the computer-executable step of removing the target program from the computer system in response to an identification that the target program comprises malicious code so that the target program cannot affect performance of subsequent programs executed by the computer system.

28. (Currently Amended) The memory storage device of Claim 26, wherein the step of collecting information about the behavior of the target program in response to virtual execution of the target program comprises storing bits that correspond to the flags in a behavior pattern register, the behavior pattern register providing memory for the behavior pattern field, the storing of the bits being completed in response to monitoring operating system calls, interrupts and I/O port read/write operations completed by the virtual machine.

29. (Currently Amended) A memory storage device comprising computer-executable steps for identifying the presence of malicious code in program code in a computer system, comprising:

~~initializing~~ building a new virtual machine for the computer system by assigning fresh physical memory to a memory array each time a target program is to be executed, the memory array functioning as memory for the virtual machine, the virtual machine comprising a complete virtual personal computer (PC) implemented by software simulating functionality of a central processing unit, [[and]] memory, [[and]] a virtual operating system simulating functionality of a multi-threaded operating system of the computer system, input/output (I/O) ports, BIOS firmware, and data areas for the virtual operating system;[[,]]

the initializing step comprising the steps of extracting the file structure of [[a]] the target program and loading the target program into the software-simulated memory of the virtual PC;

executing a target program within the virtual PC so that the target program completes a virtual execution by interacting only with an instance of the virtual operating system;

generating a behavior pattern by completing virtual execution of the entire code of the target program within the virtual PC, the behavior pattern representative of a sequence of operational functions completed by the target program during virtual execution, including at least one of virtual operating system calls, Input/Output functions and program functions supported by the target program;

upon completion of virtual execution, operating the virtual machine to compare the behavior pattern generated by virtual execution of the target program to a behavior pattern representative of operations by the malicious code to identify an occurrence of malicious code behavior; and

in the event that the comparison process results in a match representing an identification of malicious code behavior by the target program, then identifying the target program as comprising the malicious code.

30. (Currently Amended) The memory storage device of Claim 29 further comprising the computer-executable step of removing the target program from the computer system in response to an identification that the target program comprises malicious code so that the target program cannot affect performance of subsequent programs executed by the computer system.